Supreme Court, U.S.
FILED
JAN 24 2003

No. 02-969

(A)

In The
Supreme Court of the United States

ROBERT KONOP,

Petitioner,

v.

HAWAIIAN AIRLINES, INC.,

Respondent.

On Petition For A Writ Of Certiorari To The United States Court Of Appeals For The Ninth Circuit

BRIEF OF *AMICUS CURIAE* THE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PETITIONER

LEE TIEN
Senior Staff Attorney
Counsel of Record
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, California 94110
(415) 436-9333 x 102
Attorney for Amicus Curiae

COCKLE LAW BRIEF PRINTING CO. (800) 225-6964
OR CALL COLLECT (402) 342-2831

23pp

QUESTION PRESENTED

The Wiretap Act defines "interception" as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any . . . device." Federal courts, however, also require that "interception" be "contemporaneous" with the communication's transmission. Where no such requirement appears in the statutory text, have the courts acted correctly in adding this "contemporaneity" requirement to the statutory definition of "interception"?

TABLE OF CONTENTS

	Page
Table of Authorities	iii
Interest of *Amicus Curiae*	1
Summary of the Argument	2
Reasons for Granting Certiorari	5
A. There is a conflict among the circuits	6
B. The issue of law has not been, but should be, settled by this Court	8
1. The statutory scheme does not require that "interception" be "contemporaneous" with communication transmission	10
2. Petitioner's position does not unduly burden law enforcement	13
3. Decision by this Court is necessary to protect Internet privacy	15
Conclusion	18

TABLE OF AUTHORITIES

Page

CASES

Bartnicki v. Vopper, 532 U.S. 514 (2001) 6, 16

Berger v. New York, 388 U.S. 41 (1967) 16

Connecticut Nat'l Bank v. Germain, 503 U.S. 249 (1992) 10

Dalia v. United States, 441 U.S. 238 (1979) 14

Katz v. United States, 389 U.S. 347 (1967) 16

Konop v. Hawaiian Airlines, 236 F.3d 1035 (9th Cir. 2001) 3, 7, 8, 10, 11

Konop v. Hawaiian Airlines, 302 F.3d 868 (9th Cir. 2002) 3, 4, 5, 13

Konop v. Hawaiian Airlines, 262 F.3d 972 (9th Cir. 2001) 3

Kyllo v. United States, 533 U.S. 27 (2001) 8

Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994) ..... *passim*

United States v. Meriwether, 917 F.2d 955 (6th Cir. 1990) 7, 15

United States v. Moriarty, 962 F.Supp. 217 (D.Mass. 1997) 8

United States v. Smith, 155 F.3d 1051 (9th Cir. 1988) 5, 6, 7, 8

United States v. Turk, 526 F.2d 654 (5th Cir. 1976) 7, 10, 12, 13

United States v. U.S. District Court, 407 U.S. 292 (1972) 15, 16

TABLE OF AUTHORITIES – Continued

Page

CONSTITUTION

U.S. Const., Fourth Amendment 9

STATUTES

18 U.S.C. § 2510(4) 4, 10
18 U.S.C. § 2510(5)(a)(1) 4
18 U.S.C. § 2510(12) 11
18 U.S.C. § 2510(12)(D) 11
18 U.S.C. § 2511(a) 3
18 U.S.C. § 2511(1)(a) 8
18 U.S.C. § 2515 15
18 U.S.C. § 2518(10)(a) 15
18 U.S.C. § 2520 7
18 U.S.C. § 2701 ..... 4, 8, 11
18 U.S.C. § 2703 15
18 U.S.C. § 2703(a) 4, 13, 14
18 U.S.C. § 2707 7

OTHER MATERIALS

S. REP. NO. 99-541, 99th Cong., 2d Sess. (1986) 5, 16

INTEREST OF *AMICUS CURIAE*

This brief *amicus curiae* in support of petitioner Robert Konop ("Konop") is submitted by the Electronic Frontier Foundation ("EFF") pursuant to Rule 37 of this Court. Counsel for petitioner and respondent have consented to the filing of this brief, and their consent letters have been filed with the Clerk of the Court.

Amicus is a non-profit, member-supported public-interest organization dedicated to the protection of civil liberties in the high-technology arena.[1] Based in San Francisco, California, EFF has about 9000 members and maintains one of the most linked-to websites in the world at <http://www.eff.org>.

EFF and its members use the Internet extensively and seek to protect individual rights from being eroded by new technologies and by laws that, often unwittingly, impose greater burdens on or afford less protection to speech and privacy in new media. Hence EFF's interest in this case, where petitioner, an airline pilot, created a password-protected website in order to communicate privately with other pilots on labor-management issues concerning their employer, respondent Hawaiian Airlines, Inc. ("Hawaiian"), and where Hawaiian accessed petitioner's website without authorization and then acquired contents of Konop's communications. The Ninth Circuit held that Hawaiian did not "intercept" communications under the Wiretap Act.

---

[1] No counsel for any party authored this brief in whole or in part. Mr. Kevin Dailey made a monetary contribution to defray the costs of printing and submitting this brief.

If the Court does not reverse the Ninth Circuit's holding, such communication will lack the privacy it deserves, harming Konop and all others who use password-protected websites or other privacy techniques to communicate or work together privately on computer networks. More fundamentally, this Court would perpetuate the judicially legislated but statutorily unsupported definition of interception, under which a communication can only be intercepted "contemporaneously" with its transmission.

This "contemporaneity" requirement limits the Wiretap Act's applicability to Internet communications: anyone can use a device to acquire the contents of password-protected communication on a website or to acquire an e-mail's contents after the e-mail has arrived at the recipient's e-mailbox without violating the Wiretap Act, even though in both scenarios such conduct fits the statutory definition of "interception."

SUMMARY OF THE ARGUMENT

This is a case of national significance, which can either protect or erode Americans' communications privacy rights. Historically, oral and wire communications are synchronous: they occur in "real time." In contrast, Internet communications are generally asynchronous: message transmission and reception do not happen at the same time and may be separated by days, weeks or months.

The key issue is simple: does Title I of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510-2521 ("Wiretap Act")[2], only protect "live" communication against "interception" – as when a wiretapper listens to an ongoing phone conversation – or does it also protect "store-and-forward" or "leave-and-retrieve" communication like Konop's messages to his fellow pilots?

Konop's argument is also simple. He used his website to communicate privately with others; Hawaiian accessed the website without authorization and then acquired the contents of his communications. Thus, Hawaiian *accessed* Konop's private website in violation of Title II of ECPA, the Stored Communications Act ("SCA"), 18 U.S.C. § 2701(a)(2), and *intercepted* Konop's private electronic communications in violation of the Wiretap Act, 18 U.S.C. § 2511(a). Although this argument conflicted with the views of other circuit courts, it adheres to the statutory text and was initially accepted in *Konop v. Hawaiian Airlines*, 236 F.3d 1035 (9th Cir. 2001) ("*Konop I*"), *opinion withdrawn*, 262 F.3d 972 (9th Cir. 2001).

In its second decision, the Ninth Circuit reversed itself and found that Hawaiian did not intercept Konop's communications because Hawaiian did not acquire their contents during transmission. *Konop v. Hawaiian Airlines*, 302 F.3d 868 (9th Cir. 2002) ("*Konop II*"). The Ninth Circuit believed that its holding in *Konop I* conflicted with

---

[2] The federal wiretapping statute was originally created by Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub.L. No. 90-351, 82 Stat. 212. It was amended and retitled by Title I of the Electronic Communications Privacy Act of 1986, Pub.L. No. 99-508, 100 Stat. 1851.

another SCA provision, which sets forth procedures for compelling a service provider to *disclose* communication contents to the government. 18 U.S.C. § 2703(a).

Thus, this case is framed by the interrelationship of three statutory concepts: access, interception, and disclosure. EFF argues that these concepts are interrelated as follows. *Access* under the SCA occurs when a person enters a communications transmission or storage facility and is in a position to, among other things, acquire communication contents. 18 U.S.C. § 2701. *Interception* under the Wiretap Act occurs when communication contents are in fact acquired by using a device.[3] 18 U.S.C. § 2510(4). *Disclosure* under the SCA occurs when the government acquires communication contents by compelling the service provider to provide those contents to the government. 18 U.S.C. § 2703(a).

This approach, which obviates "contemporaneity," is faithful to the statutory text and dispels the illusory conflict between Konop's position and the statutory structure. The Ninth Circuit erred in *Konop II* by equating *interception by* the government (or anyone else) with *disclosure to* the government of communication contents by service providers. This equation is invalid: *interception* requires use of a device by the interceptor, but *disclosure* does not. Because *interception* procedures allow government acquisition of contents by use of a device, while *disclosure* procedures allow government acquisition of

[3] Such a device does not include equipment provided to the user or subscriber of a communications service by the communications service provider. 18 U.S.C. § 2510(5)(a)(1).

contents by compelling their production by service providers, no conflict exists: the two types of procedures regulate entirely different government conduct. In short, holding that Hawaiian intercepted Konop's communications has no untoward or unintended effects on the SCA's disclosure procedures.

REASONS FOR GRANTING CERTIORARI

This is a case of national significance for communications privacy rights in which the Ninth Circuit decision in *Konop II* conflicts with an earlier Ninth Circuit decision, *United States v. Smith*, 155 F.3d 1051 (9th Cir. 1988) (voicemail), *cert. denied*, 525 U.S. 1071 (1999), creating different approaches to the federal scheme that protects the privacy of both "live" and "store-and-forward/leave-and-retrieve" electronic communications. *Smith* also conflicts with the law of other circuits. *E.g.*, *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994). Thus, a circuit split exists under Rule 10(a) of this Court.

Moreover, this case presents an important question of federal law that has not been, but should be, settled by this Court under Rule 10(c) of this Court. Despite the growing importance of the Internet and thus asynchronous electronic communication, this Court has not yet interpreted the relationship between the Wiretap Act and the SCA as applied to electronic communications. In enacting ECPA to amend the Wiretap Act and create the SCA, Congress's main purpose was "to protect against the unauthorized interception of electronic communications." S. REP. NO. 99-541, 99th Cong., 2d Sess. at 1 (1986) ("The

bill . . . update[s] and clarif[ies] Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.").

Unfortunately, the lower courts have found the scheme confusing. *Steve Jackson Games*, 36 F.3d at 462 (federal surveillance law "famous (if not infamous) for its lack of clarity"); *Smith*, 155 F.3d at 1055 ("complex, often convoluted, area of the law"). In their confusion, the courts have mistakenly grafted upon ECPA a requirement of "contemporaneity," which is alien to the statutory text and structure. Limiting "interception" to the contemporaneous acquisition of communication contents means that anyone may use a device to acquire an e-mail's contents after the e-mail has arrived at the recipient's e-mailbox without violating the Wiretap Act, even though such conduct fits the statutory definition of "interception."

It is ironic that this unnecessary, privacy-hostile requirement has been imposed on a statute that was intended to advance with technology. Guidance from this Court is needed to restore the statute's plain text and effect Congress's yet-unrealized intent.

A. There is a conflict among the circuits.

The statutory communications privacy scheme was intended to "protect the privacy of wire, electronic, and oral communications." *Bartnicki v. Vopper*, 532 U.S. 514, 526 (2001) (internal quotation marks and citation omitted). Unfortunately, the interplay of the Wiretap Act and the SCA is notoriously confusing, hindering the scheme's power to protect privacy.

Perhaps the most troublesome issue in the scheme is also one of the most basic: what does it mean to "intercept" a communication? The answer to this question determines whether an act is subject to the Wiretap Act's strict protections or the SCA's more relaxed protections.[4]

The circuits approach this question in at least two ways. Most circuits use the Fifth Circuit's "temporal" approach: the Wiretap Act applies only when the contents of a communication are acquired contemporaneously with its transmission. *United States v. Turk*, 526 F.2d 654, 658 (5th Cir. 1976); *United States v. Meriwether*, 917 F.2d 955, 959 (6th Cir. 1990) ("Since the transmission had ceased, the subsequent retrieval of the message was not an 'interception' as contemplated by the drafters of the statute."). Conversely, under this approach the SCA applies when communications contents are acquired while they are stored. *Steve Jackson Games*, 36 F.3d at 460.

The Ninth Circuit has twice adopted a different, "qualitative" approach to the statutory scheme. In both *Smith* and *Konop I*, the Ninth Circuit rejected the argument that stored communications could not be intercepted merely because they were stored. Instead, the Ninth Circuit distinguished access and interception qualitatively: "access" is a "lesser included offense" of "interception." *Smith*, 155 F.3d at 1058. The SCA's "access" prohibition might have been violated by unauthorized use of a password to enter a voicemail system without

[4] Civil damages are substantially greater under the Wiretap Act than under the SCA. *Compare* 18 U.S.C. § 2520 *with* 18 U.S.C. § 2707.

intercepting message "contents," but actually "retriev[ing] and record[ing]" a message is an "interception." *Ibid.*

The government itself has used similar reasoning. In *United States v. Moriarty*, 962 F.Supp. 217 (D.Mass. 1997) (access to stored voicemail), the government argued that the SCA "only requires 'access,' which, by implication, does not necessitate the acquisition of the communication." *Id.* at 219. As the government put it: "a person could violate 18 U.S.C. §2701 by entering the Justice Department's computer system and altering the codes that would allow *access* to e-mail by authorized users. This would be a violation even though confidential e-mail messages were never *intercepted.* Such conduct would not violate 18 U.S.C. §2511(1)(a)." *Ibid.* (quoting government brief) (emphasis in original). The government's distinction in *Moriarty* between access and interception tracks the reasoning of *Smith* and *Konop I*.

B. The issue of law has not been, but should be, settled by this Court.

Certiorari should also be granted for the independent reason that the Ninth Circuit and other circuits have decided an important question of federal law that has not been, but should be, settled by this Court within the meaning of Rule 10(c) of this Court.

Individual privacy has suffered greatly with the advent of electronic technologies that automatically and invisibly create records of our speaking, reading, and other activities on the Internet, and with the advent of new technologies that facilitate covert surveillance in both the "virtual" and the physical world. *See Kyllo v. United States*, 533 U.S. 27, 33-34 (2001) ("It would be foolish to

contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology. . . . The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.").

Most people are only dimly aware of these threats to their privacy. Covert surveillance, unlike a physical search of a person or home, does not announce itself. Moreover, the inner workings of new technologies are almost by definition obscure to the average person; how many people can protect the privacy of their Internet browsing activities – or even realize that they might want to? Unfortunately, the law has responded to these technological changes only erratically at best.

This case is an example. When the Wiretap Act was first enacted, most of the private communication that it covered took place in real time. Even when ECPA amended the Wiretap Act and created the SCA, "store-and-forward" private communication was in its infancy. The role of "leave-and-receive" communications like e-mail has grown with the Internet. Fortunately, Congress defined "interception" in a temporally neutral way that does not disfavor electronic communications.

Unfortunately, the courts ignore Congress's plain language. They instead rely on an unnecessary judicial gloss – contemporaneity – that originated in an oral communication case but does not fit Internet communications. Limiting "interception" to contemporaneous acquisition of communication contents means that anyone may use a device to acquire an e-mail's contents after the e-mail has arrived at the recipient's e-mailbox without

violating the Wiretap Act, even though such conduct fits the statutory definition of "interception."[5]

1. The statutory scheme does not require that "interception" be "contemporaneous" with communication transmission.

The plain language of ECPA controls here. ECPA contains one definition of "intercept" with no temporal parameters. 18 U.S.C. § 2510(4) (defining "intercept" as "the [] acquisition of the contents of any wire, electronic, or oral communication through the use of any [] device"); *Konop I*, 236 F.3d at 1044 (no reference to contemporaneity in legislative history). Even the Fifth Circuit recognized that the definition of "intercept" contains "[n]o explicit limitation of coverage to contemporaneous 'acquisition'" of communication contents. *Turk*, 526 F.2d at 658.

It is a "cardinal canon" of statutory construction "that a legislature says in a statute what it means and means in a statute what it says there." *Connecticut Nat'l Bank v. Germain*, 503 U.S. 249, 253-254 (1992). Had Congress meant to limit interception to "contemporaneous" acquisition of communication contents, it could easily have done so.

---

[5] As the Ninth Circuit put it: "A requirement that transmission and acquisition be contemporaneous would be fatal to Konop's claim that Hawaiian violated the Wiretap Act by gaining unauthorized access to his website. There is ordinarily a period of latency between the initial transmission of information for storage on a web server, and the acquisition of that information by its recipients. If interception requires that acquisition and transmission occur contemporaneously, then unauthorized downloading of information stored on a web server cannot be interception." *Konop I*, 236 F.3d at 1043.

The statutory structure confirms that "contemporaneity" is unnecessary. The SCA prohibits unauthorized "access" to a "facility" that allows a person to "obtain[ ], alter[ ], or prevent[ ] authorized access to a wire or electronic communication while it is in electronic storage." 18 U.S.C. § 2701. This language says nothing about "acquisition" of communications "contents" by "device," which are the defining features of "interception." Indeed, the word "contents" appears nowhere in the provision.

The statutory language also confirms that "storage" is irrelevant to the question of whether electronic communications are intercepted. First, nothing in 18 U.S.C. § 2510(12)'s definition of "electronic communication" suggests that communication in "electronic storage" cease to be "electronic communication." Second, Congress in 1996 excluded one type of stored communication from this definition: "electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds." 18 U.S.C. § 2510(12)(D).[6] That Congress did so again indicates that stored electronic communication, in general, remains "electronic communication." Thus, it cannot disturb the statutory scheme to recognize that the Wiretap Act covers interception of stored communication because 18 U.S.C. § 2701 does not cover interception.

---

[6] As the Ninth Circuit observed in *Konop I*, the conference report indicates that Congress understood this point: "[The amendment] will allow law enforcement to obtain [stored] bank records through the usual grand jury subpoena, or other court order procedure, *without requiring a wiretap order* for these purposes." *Konop I*, 236 F.3d at 1043 (citation omitted) (emphasis added).

Much of the confusion here arises from the Fifth Circuit's misapplication of *Turk* in *Steve Jackson Games*. Properly understood, *Turk* is about whether police "intercept" when they listen to an oral communication that someone else independently intercepted. In *Turk*, police seized and listened to a pre-recorded tape of a conversation lawfully intercepted by one of the conversation's participants. The Fifth Circuit was concerned that absurd results would follow if the officers' replaying the tape were an interception. Each time they listened to the tape, it would be another interception; even if only the first listening were an interception, it would be odd to say that there could be a room filled with officers, with only first-time listeners intercepting. *Turk*, 526 F.2d at 658 n. 4.

To address these concerns, *Turk* required "participation by the one charged with an 'interception' in the contemporaneous acquisition of the communication through the use of a device." *Id.* at 658 & n.3 ("'interception' requires . . . involvement in the initial use of the device contemporaneous with the communication to transmit or preserve the communication"). The officers used no device to seize the communication; they acquired the contents after the original lawful interception.

Turk did not rule on "the precise temporal parameters" of interception, *id.* at 659, which makes perfect sense. Oral communication is not delivered by service providers. Intercepting an oral communication is always contemporaneous; otherwise, the words vanish into thin air. Nothing in *Turk* changes if "contemporaneity" is deleted. The crucial element in *Turk* was not contemporaneity, but the officers' uninvolvement in intercepting the communication.

Steve Jackson Games presented an entirely different situation: the government agents seized, read and destroyed 162 items of unread, private e-mail. *Steve Jackson Games*, 36 F.3d at 459. The issues that plagued the *Turk* court were absent. But the Fifth Circuit took *Turk*'s notion of "contemporaneity," which played no essential part of *Turk*'s reasoning, and unthinkingly applied it to e-mail.

2. Petitioner's position does not unduly burden law enforcement.

The Ninth Circuit decision to reverse itself was based largely on its perception that the qualitative approach would unduly burden law enforcement.

> Section 2703(a) of the SCA details the procedures law enforcement must follow to access the contents of stored electronic communications, but these procedures are considerably less burdensome and less restrictive than those required to obtain a wiretap order under the Wiretap Act. Thus, if Konop's position were correct and acquisition of a stored electronic communication were an interception under the Wiretap Act, the government would have to comply with the more burdensome, more restrictive procedures of the Wiretap Act to do exactly what Congress apparently authorized it to do under the less burdensome procedures of the SCA. Congress could not have intended this result.

Konop II, 302 F.3d at 879 (internal citation omitted). The Ninth Circuit concluded that, while a broad construction of the Wiretap Act was "not without appeal, the language and structure of the ECPA demonstrate that Congress considered and rejected this argument." *Id.*, at 879 n. 6.

This erroneous conclusion is based on a misreading of the statutory text. The qualitative approach distinguishes *access* from *interception*. Neither term, however, is implicated by the SCA's provisions for compelled provider *disclosure* of communications contents to the government. Konop's position is about interception, not disclosure.

The Ninth Circuit confused provider disclosure with government interception. In both scenarios the government acquires communications contents. But § 2703(a) regulates one mode of government acquisition: compelled *disclosure* of communications contents to the government from the provider. The Wiretap Act regulates another mode of contents acquisition: *interception*, which requires using a device and involves no disclosure from (and possibly no involvement by[7]) the provider.

The flaw in the Ninth Circuit's reasoning can easily be seen. The authorization government must have to compel *disclosure* from the service provider is not the same as the authorization government must have to *intercept* communications. The SCA's "less burdensome procedures" apply when the government seeks to compel disclosure of communications contents from a service provider. In *Steve Jackson Games*, for instance, the government might

[7] For example, government agents may covertly enter premises and install an electronic listening device in order to execute a valid interception order. *Dalia v. United States*, 441 U.S. 238, 257-258 (1979). Presumably, they also could covertly enter an electronic communication service provider's premises and install equipment like the Federal Bureau of Investigation's "Carnivore" in order to execute a valid interception order.

properly have used a search warrant to compel the bulletin board service operator to disclose the e-mails.

The situation is different when government seeks to use a device to acquire communications contents on its own. Imagine if the government "cracked" into Konop's password-protected website and acquired the contents of his communications. The Wiretap Act's "more burdensome, more restrictive procedures" apply when the government engages in such "self-help," and an interception order would be needed.

In short, 18 U.S.C. § 2703 regulates disclosure, not interception. Accepting Konop's position and holding that Hawaiian intercepted Konop's communications does not supplant the SCA; the government does not need an interception order to compel disclosure of communication contents from a service provider. Konop's position is entirely consistent with the text of the statutory scheme and conflicts with neither the statutory text nor Congressional intent.[8]

3. Decision by this Court is necessary to protect Internet privacy.

ECPA was intended to protect constitutional rights. Its predecessor was written "to meet the constitutional requirements" governing wiretapping. *See United States v.*

---

[8] Congress protected electronic communication less than wire communication in a very clear way: there is a statutory suppression remedy for fruits of unlawful telephone wiretapping. 18 U.S.C. § 2515, § 2518(10)(a). No such remedy exists for unlawful interception of electronic communication. *Meriwether*, 917 F.2d at 960.

U.S. District Court, 407 U.S. 292, 302 (1972) (citing *Berger v. New York*, 388 U.S. 41 (1967), and *Katz v. United States*, 389 U.S. 347 (1967)). That intent was carried forward when Congress enacted ECPA. S. REP. NO. 99-541, at 5 (federal law should "advance with technology to ensure the continued vitality of the Fourth Amendment."). Protecting communications privacy against "official eavesdropping" also protects free speech. *U.S. District Court*, 407 U.S. at 314-315; *Bartnicki*, 532 U.S. at 533.

Unfortunately, ECPA has not been interpreted to promote these rights. As *amicus* has explained above, different modes of communication have different temporal characteristics. Much communication today does not take place in real time; it is of the "store-and-forward" or "leave-and-retrieve" variety. But the courts erroneously read the "contemporaneity" requirement into the statutory definition of "interception," and now refuse to correct that error. This Court should clarify the meaning of "interception" in line with the rights at stake: speech and privacy. Happily, this clarification can be accomplished simply by following the statutory text.

The qualitative approach better protects these rights than the competing temporal approach. By treating unauthorized access as a lesser included offense of unauthorized interception, the severity of the offense is more closely tied to the magnitude of privacy intrusion and speech chill. Acquiring e-mail contents from storage violates one's privacy more than merely "cracking" into an e-mail system without acquiring e-mail contents.

The temporal approach, on the other hand, produces perverse results for communications privacy. As noted earlier, limiting "interception" to contemporaneous acquisition of communication contents means that anyone may

use a device to acquire an e-mail's contents after the e-mail has arrived at the recipient's e-mailbox without violating the Wiretap Act, even though such conduct fits the statutory definition of "interception" and invades privacy just as much as a "live" interception.

Amicus has shown, moreover, that the qualitative approach does not burden law enforcement. The SCA's disclosure provisions are unaffected. Law enforcement does not need an interception order to compel disclosure of stored electronic communication contents, because compelling disclosure from providers is not interception.

Finally, websites are an increasingly important medium for private electronic communication. In 1986, few could have imagined the Internet, much less its use for private communication like that between Konop and his fellow pilots. Konop's website is but one example of the growing use of websites for private electronic communication. Such websites are like private rooms in cyberspace for holding meetings or conversations. *See, e.g.*, <http://intranets.com/> ("A private space on the web where your group can easily access and share documents, calendars and event information"); <http://www.superfamily.com/> ("At SuperFamily.com, your entire family can share a password protected website together from anywhere in the world.").

This is a case where the courts have shrunk statutorily guaranteed privacy by rewriting a law that by its terms does not do so. This Court can protect Internet speech and privacy simply by instructing the lower courts to adhere to the statute's plain text.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted,

LEE TIEN
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, California 94110
(415) 436-9333 x 102